IN THE CLAIMS:

Please cancel claims 4-5, 15-16 and 23-40 without prejudice to or disclaimer of the subject matter recited therein.

Please amend claims 1, 6, 12-14 and 17-21 as follows:

LISTING OF CURRENT CLAIMS

1. (Currently Amended) A digital information protecting method for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used, both the author computer and the client computer comprising a predetermined information processing software to process the piece of digital information, the information processing software of the author computer comprising a plurality of universal keys with encoded serial number, the method comprising:

in the author computer:

receiving a content key from a server and encrypting the piece of digital information by the content key;

choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key;

storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information; and

~~encrypting the content key by a predetermined key encrypting process;~~

transmitting the encrypted digital information and the encrypted content key to the client computer; and

in the client computer:

decrypting the encrypted content key by a corresponding predetermined key decrypting process; and

decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer.

2. (Original) The digital information protecting method of claim 1, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server.

3. (Original) The digital information protecting method of claim 2, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

Claims 4-5. (Canceled)

6. (Currently Amended) The digital information protecting method of claim 51, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission.

7. (Original) The digital information protecting method of claim 6, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation.

8. (Original) The digital information protecting method of claim 7, wherein the key decrypting process is executed the following steps by the information processing software of the client computer:

getting a corresponding universal key according to serial number stored in the header; and

decrypting the content key by the universal key.

9. (Original) The digital information protecting method of claim 8, wherein the information processing software of the client computer downloads the universal key from the server according to the serial number.

10. (Original) The digital information protecting method of claim 8, wherein the information processing software of the client computer comprises a plurality of universal keys, the information processing software of the client computer chooses corresponding universal key according to the serial number.

11. (Original) The digital information protecting method of claim 1, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard (AES) method.

12. (Currently Amended) A digital information protecting system for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used, both the author computer and the client computer comprising a predetermined information processing software to process the piece of digital information, the system comprising:

a first digital information process software, being set in the author computer, the information processing software of the author computer comprising a plurality of universal keys with encoded serial number, the first digital information process software comprising:

a content encrypting module, for

receiving a content key from a server; and

encrypting the piece of digital information by the content key; and

a key encrypting module, for

~~encrypting the content key by a predetermined key encrypting process; and~~

choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key;

storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information; and

transmitting the encrypted digital information and the encrypted content key to the client computer; and

a second information process software, setting in the client computer, comprising:

a key decrypting module, for

decrypting the encrypted content key by a corresponding predetermined decrypting process; and

a content decrypting module, for

decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer.

13. (Currently Amended) The digital information protecting system of claim ~~14~~12, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server.

14. (Currently Amended) The digital information protecting system of claim ~~15~~13, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

Claims 15-16. (Canceled)

17. (Currently Amended) The digital information protecting system of claim ~~18~~12, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission.

18. (Currently Amended) The digital information protecting system of claim ~~19~~17, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation.

19. (Currently Amended) The digital information protecting system of claim ~~20~~18, wherein the key decrypting process is executed the following steps by the information processing software of the client computer:

getting a corresponding universal key according to serial number stored in the header; and

decrypting the content key by the universal key.

20. (Currently Amended) The digital information protecting method of claim ~~21~~19, wherein the information processing software of the client computer downloads the universal key from the server according to the serial number, the information processing software of the client computer chooses corresponding universal key according to the serial number.

21. (Currently Amended) The digital information protecting method of claim ~~21~~12, wherein the information processing software of the client computer comprises a plurality of universal keys.

22. (Original) The digital information protecting system of claim 14, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard (AES) method.

Claims 23-40. (Canceled)